

07.03.00

FISH & RICHARDSON P.C., P.A.

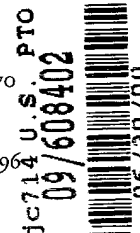
A

3300 Dain Rauscher Plaza
60 South Sixth Street
Minneapolis, Minnesota
55402

Telephone
612 335-5070

Facsimile
612 288-9696

Web Site
www.fr.com



June 30, 2000

Attorney Docket No.: 10559-225001

Box Patent Application
Commissioner for Patents
Washington, DC 20231

Presented for filing is a new patent application claiming priority from a provisional patent application of:

Applicant: ERNIE F. BRICKELL AND WESLEY DEKLOTZ

Title: DIGITAL CREDENTIAL USAGE REPORTING

Enclosed are the following papers, including those required to receive a filing date under 37 CFR 1.53(b):

	Pages
Specification	14
Claims	12
Abstract	1
Declaration	[To be Filed at a Later Date]
Drawing(s)	4

Enclosures:

— Postcard.

Under 35 USC §119(e)(1), this application claims the benefit of prior U.S. provisional application 60/199,220, filed April 24, 2000.

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No. EL640041818US

Date of Deposit June 30, 2000

I hereby certify that this correspondence is being deposited with the United States Postal Service as **express mail** with sufficient postage on the date indicated above and is addressed to the Assistant Commissioner for Patents, Box Patent Application, Washington, D.C. 20231

Vince Defante



Frederick P. Fish
1855-1930

W.K. Richardson
1859-1951



BOSTON

DALLAS

DELAWARE

NEW YORK

SAN DIEGO

SILICON VALLEY

TWIN CITIES

WASHINGTON, DC

FISH & RICHARDSON P.C., P.A.

Commissioner for Patents
June 30, 2000
Page 2

Basic filing fee	\$690
Total claims in excess of 20 times \$18	\$648
Independent claims in excess of 3 times \$78	\$390
Fee for multiple dependent claims	\$0
Total filing fee:	\$1728

Under 37 CFR §1.53(d), no filing fee is being paid at this time.

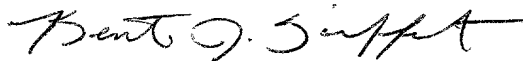
If this application is found to be incomplete, or if a telephone conference would otherwise be helpful, please call the undersigned at (612) 335-5070.

Kindly acknowledge receipt of this application by returning the enclosed postcard.

Please send all correspondence to:

SCOTT C. HARRIS
Fish & Richardson P.C.
4350 La Jolla Village Drive, Suite 500
San Diego, CA 92122

Respectfully submitted,



Kent J. Sieffert
Reg. No. 41,312
Enclosures
KJS/jlm
60016454.doc

APPLICATION
FOR
UNITED STATES LETTERS PATENT

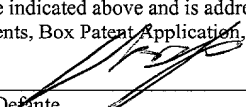
TITLE: DIGITAL CREDENTIAL USAGE REPORTING
APPLICANT: ERNIE F. BRICKELL AND WESLEY DEKLOTZ

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No. EL640041818US

June 30, 2000
Date of Deposit

I hereby certify that this correspondence is being deposited with the United States Postal Service as **express mail** with sufficient postage on the date indicated above and is addressed to the Assistant Commissioner for Patents, Box Patent Application, Washington, D C 20231


Vince Defante

DIGITAL CREDENTIAL USAGE REPORTING

Priority is claimed from United States provisional patent application serial no. 60/199,220, filed April 24, 2000.

BACKGROUND

5 Cryptography provides the basis for a number of privacy and authentication mechanisms used in computer-based systems. One such mechanism is a digital signature, which is often used to authenticate the sender of an electronic message. To create a digital signature, the sender first creates a private
10 signature key and a corresponding public verification key. To sign a message or other document, the sender performs a computation that takes as input the message and the private signature key and produces as output a digital signature for that message. To verify a digital signature, a receiver
15 performs a computation that takes as input the message, the digital signature for that message, and the public verification key, and produces as output either "signature verified" or "signature failed to verify."

20 In order to facilitate the authentication of a digitally signed document, the receiver must be assured that the public verification key that is used to verify the signature is indeed the public verification key belonging to the sender of the message. Typically, the receiver will obtain a digital

certificate, which contains the identity of the sender, the public verification key of the sender, and other information. Typically, this digital certificate is digitally signed by a certification authority. Other mechanisms are also used for establishing the correspondence between an identity and a public verification key such as an entry in a database.

DESCRIPTION OF DRAWINGS

Figure 1 is a block diagram illustrating one example of a system that monitors the usage of digital credentials.

Figure 2 is a flow chart illustrating one example of a process for monitoring the usage of digital credentials.

Figure 3 is an example activity log.

Figure 4 is a block diagram illustrating a computer suitable for implementing embodiments of the invention.

DESCRIPTION

A user's "digital credential", as used herein, refers to the security mechanisms associated with the user's identity. For example, a user's digital credential can include one or more digital signature keys relating to one or more digital certificates. In addition, a user's digital credential can be any other suitable cryptographic security mechanism, such as a mechanism for use in a proprietary cryptographic scheme.

Validating a user's digital credential, therefore, can include one or more tasks. Examples include verifying that the user's digital signature is valid using the public key in the user's digital certificate and validating the digital certificate, which can include several additional tasks such as using a key of the certification authority to validate that the digital signature on the digital certificate is valid, verifying that the digital certificate has not been revoked or suspended, and validating the key of the certification authority.

Figure 1 is a block diagram illustrating one example of a system 2 that tracks the usage of digital credentials, generates activity reports, and identifies potential fraudulent activities or other misuse. As explained in detail below, system 2 allows timely detection of fraudulent activity or general misuse of digital credentials.

Web browser 12, such as Internet Explorer™ from Microsoft™ Corporation of Redmond, Washington, executes in an operating environment provided by computing device 4A and allows an owner of digital credential 16 to remotely access online services 6 via network 28. Generally, online services 6 represent web-based venues that support secure electronic transactions. For example, online services 6 can be web-based retailers of consumer products such as books, movies,

software, toys, games and the like. Alternatively, online services 6 can be business-to-business web sites such as online marketplaces for medical and other supplies. Other examples include online banking institutions, brokerage firms, and health care services. Similarly, authorized delegates of the user use web browsers (not shown) executing on computing devices 4B through 4M to access online services 6 and conduct secure transactions using a digital credential that has been authorized by the user to act on behalf of the user for specified uses.

Computing devices 4 represents general purpose computing systems suitable for interacting with network 28. One example of a suitable computing device 4 is a personal computer. In addition, each computing device 4 can be a laptop computer, a handheld computer, a personal digital assistant (PDA), such as a Palm™ organizer from Palm Inc. of Santa Clara, California, or even a network-enabled cellular telephone. Network 28 represents any communication network, such as a packet-based digital network like the Internet.

Credential service provider (CSP) 8 provides a central service by which a user can manage his or her digital credentials. More specifically, CSP 8 allows a user to request a digital credential, revoke a digital credential and define one or more delegates that are authorized to use their

own digital credential to act in behalf of the user for specified functions.

In order to obtain digital credential 16, the user directs web browser 12 to CSP 8, generates a private signature key and a public verification key, and requests a digital certificate. The user submits the public verification key and a variety of information, such as name and address, that is validated during the application process.

CSP 8 submits the information to credential issuing service (CIS) 22 that, as a certificate authority, issues a corresponding digital credential 16, including a digital certificate and signature key, and records the owner information in owner database 24. In this fashion, the user becomes the "owner" of his or her digital credential 16. After CIS 22 issues digital credential 16 the owner can access CSP 8 and designate one or more authorized delegates.

The owner uses digital credential 16 to securely access online services 6, present digitally signed documents and otherwise conduct secure transactions. In one configuration, web browser 12 establishes a secure communication link with a web server at one of the online services 6 using a secure communications protocol, such as the Secure Socket Layer (SSL). When accessed, the web server issues a "challenge" to web browser 12. Web browser 12 responds by signing the

challenge with his private signature key and communicating digital credential 16 and the signed challenge to online service 6. In another configuration, web browser 12 uses his private signature key to digitally sign a document presented to online server 6, such as when the owner or delegate is submitting a confidential medical diagnosis or a prescription request to a web-based health care service.

Online services 6 can opt to validate digital credential 16 directly, such as by verifying the digital signatures using the public key and by checking a local database to verify the association between the public key and the user. However, online services 6 can also communicate the digital credential 16 to credential verification service 10 (CVS) for verification. In one configuration, online services 6 validate transactions of low monetary value locally and use CVS 10 to validate high value transactions.

To validate a digital credential 16, CVS 10 receives the digital credential, such as the digital signature and the digital certificate, from online services 6 and interacts with CIS 22. CVS 10 accesses CIS 22 to obtain the public key for CIS 22, as a certificate authority, and verifies the digital signature. Next, CVS 20 accesses CIS 22 to determine whether digital credential 16 has been revoked, as indicated by

certificate repository 26. CVS 20 stores the result of the verification, whether successful or not, in activity log 20.

In one configuration, CSP 8 allows the user to generate a number of digital signature keys associated with his identity and assign a "friendly name" to each key. For example, the user may assign names such as: Office Key, Home Key, Portable Key. As described below, this allows the user to more readily track usage of the digital signature keys.

System 2 incorporates many features that allow an owner or delegate to detect unauthorized use of the digital signature key in the event digital signature key is misappropriated or otherwise misused. For example, when verifying digital signature during each secure transaction, CVS 10 can automatically send an activity report to web browser 12, which can display the activity report to the user. In this fashion the user can readily identify whether the digital signature key is being misused.

In addition, the owner or delegate can access CSP 8 and request an activity report that details any usage of digital signature key. Upon receiving such a request, CSP 8 communicates the request directly to CVS 10. CVS 10 examines activity log 20, extracts the relevant activity information, formulates a report and communicates the report to CSP 8. CSP 8 electronically presents the report to the user via network

22. The owner or delegate can also configure CSP 8 to periodically generate the report and electronically mail the report to the user. Alternatively, CSP 8 can mail a physical copy of the report to the user.

5 In addition to the above-described techniques by which an owner or delegate can detect misuse of digital credential, fraud detection module 18 of CVS 10 applies fraud detection techniques to activity log 20 in order to automatically identify misuse. As described in detail below, fraud
10 detection module 18 analyzes activity log 20 to identify any unusual patterns that may indicate misuse.

Figure 2 is a flow chart illustrating a process 30 further illustrating how system 2 monitors the usage of digital signature keys and identifies potential fraudulent
15 activities or general misuse. Each online service 6 processes secure transactions by communicating digital credential 16 to CVS 10 for verification (32). As described above, CVS 10 cooperates with CIS 22 to verify digital credential 16 including determining whether digital credential 16 is
20 revoked. In one configuration, however, online services validate the digital credential and communicate transaction information to CVS 10.

CVS 10 stores the result of each verification in activity log 26 (34). In addition, CVS 10 stores relevant transaction

information such as a date and time of the transaction, the online service 6 that is involved in the transaction, the type of transaction, the device used to access the online service 6, such as a laptop computer, cell phone or a PDA, the value of the transaction, and location and position information, such as an IP address or a name of computing device 4.

In order to facilitate the timely identification of misuse of digital credential 16, CVS 10 generates activity reports that detail the information stored in activity log 20 (26). As discussed above, CVS 10 generates the activity reports in a variety of ways and at a variety of times. For example, CVS 10 can automatically generate an activity report when handling each verification request, thereby frequently providing the information to the user. In addition, CVS 10 can periodically generate activity reports or upon request by the owner.

CVS 10 also tailors each activity report to the requestor such that the owner of digital credential 16 can view all activity, including any activity by the delegates. An individual delegate, however, can only view activity reports that list his or her activity.

Fraud detection module 18 of CVS 10 analyzes activity log 20 to identify any unusual patterns in order to identify fraudulent activities. For example, a significant increase in

the number or the size of the transactions can indicate misuse. A change in the types of transactions can indicate misuse. In addition, any indication that digital signature key 16 is suddenly being used from a different computing device, such as a change from a frequently used internet protocol (IP) address to a previously unused IP address, can also indicate misuse. Upon detecting potential misuse, CVS 10 communicates an activity report to the owner alerting him or her of the activity. In this manner, the owner can readily determine whether any fraudulent activity or general misuse has indeed occurred and the extent of the activity.

If the owner determines that unauthorized activities have indeed occurred, the owner can access CSP 8 and revoke digital credential 16. For example, the owner can revoke the associated digital certificate. Alternatively, the owner can create a new private signature key and a new public verification key and sign this public verification key with the old private signature key. System 2 can issue a new digital certificate for this new verification key. CSP 8 communicates the revocation to CIS 22, which updates the status of digital credential 16 in certificate repository 26, thereby causing any future verifications by CVS 10 of the digital credential to fail. Thus, the owner can immediately stop the fraudulent activity.

In addition, the activity report can be provided to an authorized operator of CSP 8 of CVS 10. Furthermore, an activity report detailing activity at a specific online service 6 can be generated and provided to an authorized operator at the online service.

It this manner, system 2 helps detect unauthorized use of the digital signature key in the event digital signature key is misappropriated. These features are especially advantages to professional services such as the healthcare profession.

To further illustrate these benefits, consider a healthcare professional accessing a healthcare oriented online service and requesting access to healthcare information or seeking to submit a prescriptions or diagnosis. The online service communicates transaction information describing the access request and the medical professional's digital credential to the central credential verification service. Upon receiving a verification result from the credential verification service, the healthcare oriented service provides access to the medical records. Subsequently, the healthcare oriented service receives an activity report from the credential verification service and provides the report to healthcare professional.

Figure 3 is an example activity report 30 generated by CVS 10. Activity report 30 lists the activities logged in activity log 20, broken down by owner and delegate. For each

authentication request, the example activity report 40 lists the date and time, the online service involved in the transaction, the name of the computing device 4 used by the user to originate the transaction, the value of the transaction, the type of the transaction, and the authentication result.

Figure 4 illustrates a programmable computing system (system) 100 that provides an operating environment suitable for use as a computing device 4 or as a server within CSP 8, CVS 10 or CIS 22. The system 100 includes a processor 112 that represents any suitable microprocessor such as the PENTIUM® family of microprocessors manufactured by the Intel Corporation of Santa Clara, California. Other examples include the MIPS® family of microprocessors, the POWERPC® family of microprocessors from both the Motorola Corporation and the IBM Corporation, the PRECISION ARCHITECTURE® family of microprocessors from the Hewlett-Packard Company, the SPARC® family of microprocessors from the Sun Microsystems Corporation, or the ALPHA® family of microprocessors from the Compaq Computer Corporation. In various configurations, system 100 represents any server, personal computer, laptop or a hand-held PC, a personal digital assistant (PDA) or a network-enabled cellular phone.

System 100 includes system memory 113, including read only memory (ROM) 114 and random access memory (RAM) 115, which is connected to the processor 112 by a system data/address bus 116. Input/output bus 118 is connected to the data/address bus 116 via bus controller 119. In one embodiment, input/output bus 118 is implemented as a standard Peripheral Component Interconnect (PCI) bus. The bus controller 119 examines all signals from the processor 112 to route the signals to the appropriate bus. Signals between the processor 112 and the system memory 113 are merely passed through the bus controller 119. However, signals from the processor 112 intended for devices other than system memory 113 are routed onto the input/output bus 118.

Various devices are connected to the input/output bus 118 including hard disk drive 120, floppy drive 121 that is used to read floppy disk 151, and optical drive 122, such as a CD-ROM drive that is used to read an optical disk 152. The video display 124 or other kind of display device is connected to the input/output bus 118 via a video adapter 125.

Users enter commands and information into the system 100 by using a keyboard 140 and/or pointing device, such as a mouse 142, which are connected to bus 118 via input/output ports 128. Other types of pointing devices (not shown) include track pads, track balls, joysticks, data gloves, head

trackers, and other devices suitable for positioning a cursor on the video display 124. System 100 also includes a modem 129 that is typically used to communicate over wide area networks (not shown), such as the Internet using either a
5 wired or wireless connection.

Software applications 136 and data are typically stored via one of the memory storage devices, which may include the hard disk 120, floppy disk 151, CD-ROM 152 and are copied to RAM 115 for execution. In one embodiment, however, software
10 applications 136 are stored in ROM 114 and are copied to RAM 115 for execution or are executed directly from ROM 114.

In general, the operating system 135 executes software applications 136 and carries out instructions issued by the user. The Basic Input/Output System (BIOS) 117 for the system
15 100 is a set of basic executable routines that have conventionally helped to transfer information between the computing resources within the system 100. Operating system 135 or other software applications 136 use these low-level service routines. In one embodiment system 100 includes a
20 registry (not shown) that is a system database that holds configuration information for system 100.

The invention has been described in reference to a variety of embodiments. These and other embodiments are within the scope of the following claims.

What is claimed is:

1 1. A method comprising:

2 verifying a use of a digital credential; and
3 storing a result of the verification in an activity
4 log.

1 2. The method of claim 1 further including storing
2 transaction information in the activity log.

1 3. The method of claim 2, wherein the transaction
2 information includes at least one of a message that was
3 signed using a digital signature key of the digital
4 credential, a value of a transaction, an online service,
5 an internet protocol (IP) address, a date of the
6 transaction and a time of the transaction.

1 4. The method of claim 1 further including generating an
2 activity report from the activity log, wherein the
3 activity report lists the stored verification results.

1 5. The method of claim 4 further including associating a
2 name to a digital signature key of the digital
3 credential, wherein the activity report lists the name of
4 the digital signature key.

1 6. The method of claim 4, wherein generating the activity
2 report includes generating the activity report upon
3 request by an owner of the digital credential.

1 7. The method of claim 4, wherein generating the activity
2 report includes generating the activity report each time
3 the digital credential is verified.

1 8. The method of claim 4, wherein generating the activity
2 report includes generating a report periodically.

1 9. The method of claim 1 further including analyzing the
2 activity log to detect misuse of the digital credential.

1 10. The method of claim 6, wherein generating the activity
2 report includes listing activity for a plurality of
3 digital signature keys associated with the owner.

1 11. The method of claim 1 further comprising:
2 authorizing one or more delegates to use a delegated
3 digital credential to act on behalf of the owner of the
4 digital credential for specified functions, wherein
5 verifying the use of the digital credential includes
6 determining whether the delegated digital credential was
7 authorized for the specific use.

1 12. The method of claim 4, wherein generating an activity
2 report includes activity reports of the delegates of the
3 user.

1 13. An article comprising a computer-readable medium having
2 computer-executable instructions stored thereon for
3 causing a computer to:
4 verifying a use of a digital credential; and
5 storing a result of the verification in an activity
6 log.

1 14. The article of claim 13, wherein the computer-executable
2 instructions cause the computer to store transaction
3 information in activity log.

1 15. The article of claim 14, wherein the transaction
2 information includes at least one of a message that was
3 signed using a digital signature key of the digital
4 credential, a transaction value, an online service
5 processing the transaction, an internet protocol (IP)
6 address of a computing device originating the
7 transaction, the date of the transaction and the time of
8 the transaction.

1 16. The article of claim 13, wherein the computer-executable
2 instructions cause the computer to generate an activity

report from the activity log, wherein the activity report lists the stored verification results.

17. The article of claim 16 and further including associating a name to a digital signature key of the digital credential, wherein the activity report lists the name of the digital signature key.

18. The article of claim 16, wherein the computer-executable instructions cause the computer to generate the activity report upon receiving a request by an owner of the digital credential, periodically, or when the digital credential is verified.

19. The article of claim 13, wherein the computer-executable instructions cause the computer to analyze the activity log to detect misuse of the digital credential.

20. The article of claim 17, wherein the computer-executable instructions cause the computer to list in the activity report activity for a plurality of digital signature keys associated with the owner according to the name of the digital signature key.

21. The article of claim 20, wherein the computer-executable instructions cause the computer to authorize one or more delegates to use a delegated digital credential to act on

4 behalf of the owner of the digital credential for
5 specified functions and determine whether the delegated
6 digital credential was authorized for the specific use.

1 22. The article of claim 21, wherein the computer-executable
2 instructions cause the computer to generate activity
3 reports of the delegates.

1 23. A system comprising:

2 a server to verify digital credentials; and
3 an activity log coupled to the server to store
4 results from the verification.

1 24. The system of claim 23, wherein the activity log is
2 configured to store transaction information for each
3 authentication result.

1 25. The system of claim 24, wherein the transaction
2 information includes at least one of a digitally signed
3 message, a date of the transaction, a value of the
4 transaction, an online service requesting the
5 authentication, an internet protocol (IP) address, a
6 value of the transaction, and a time of the transaction.

1 26. The system of claim 23, and further comprising an owner
2 database to store information of an owner of the digital
3 credential and owner-approved delegates.

1 27. An article comprising a computer-readable medium having
2 data structures stored thereon comprising:

3 a first data field to store a result from an
4 verification of a digital credential; and

5 a plurality of data fields to store transaction
6 information relating to each verification result.

1 28. The article of claim 27, wherein the plurality of data
2 fields store at least one of a digitally signed message,
3 a date of the transaction, a time of the transaction, a
4 value of the transaction, an online service, an internet
5 protocol (IP) address of a computing device originating
6 the transaction, and goods or services involved in the
7 transaction.

1 29. The article of claim 27, wherein the data structures
2 further include a plurality of data fields to store owner
3 and delegate information.

1 30. A method comprising:
2 receiving information describing a use of a digital
3 credential;
4 storing the use information in an activity log; and
5 generating an activity report based on activity log.

1 31. The method of claim 30, wherein the use information
2 includes transaction information.

1 32. The method of claim 30, wherein the use information
2 includes verification information for the digital
3 credential.

1 33. The method of claim 31, wherein the transaction
2 information includes at least one of a message that was
3 signed, a transaction value, an online service, an
4 internet protocol (IP) address, a value of the
5 transaction, a date of the transaction and a the time of
6 the transaction.

1 34. The method of claim 30, wherein the digital credential
2 includes a digital signature key, and further wherein
3 generating the activity report includes associating a
4 name to the digital signature key and listing the name of
5 the digital signature key.

1 35. The method of claim 30, wherein generating the activity
2 report includes generating the activity report upon
3 request by an owner of the digital credential.

1 36. The method of claim 30, wherein generating the activity
2 report includes generating the activity report each time
3 the digital credential is verified.

1 37. The method of claim 30, wherein generating the activity
2 report includes generating a report periodically.

1 38. The method of claim 30 further including analyzing the
2 activity log to detect misuse of the digital credential.

1 39. The method of claim 35, wherein generating the activity
2 report includes listing activity for a plurality of
3 digital signature keys associated with the owner.

1 40. The method of claim 30 further comprising:
2 authorizing one or more delegates to use a delegated
3 digital credential to act on behalf of the owner of the
4 digital credential for specified functions, wherein
5 verifying the use of the digital credential includes
6 determining whether the delegated digital credential was
7 authorized for the specific use.

1 41. The method of claim 30, wherein generating an activity
2 report includes activity reports of the delegates of the
3 user.

1 42. A method comprising:
2 storing use information for a digital credential of
3 a user;
4 processing the use information to detect misuse; and
5 generating an alert when misuse is detected.

1 43. The method of claim 42, wherein generating an alert
2 includes generating an activity report based on the use
3 information.

1 44. The method of claim 42, wherein generating an alert
2 includes alerting a credential service provider.

1 45. The method of claim 42, wherein the use information
2 includes transaction information.

1 46. The method of claim 42, wherein the use information
2 includes verification information for the digital
3 credential.

1 47. The method of claim 45, wherein the transaction
2 information includes at least one of a message that was
3 signed, a transaction value, an online service, an
4 internet protocol (IP) address, a value of the
5 transaction, a date of the transaction and a the time of
6 the transaction.

1 48. A method comprising:
2 receiving transaction requests from a plurality of
3 users, wherein the transaction requests include digital
4 credentials for the users;
5 processing the transaction requests; and

6 communicating transaction information to a central
7 service, wherein the transaction information includes the
8 digital credentials of the users.

1 49. The method of claim 48, wherein processing the
2 transaction requests includes communicating the digital
3 credentials to the central service for verification.

1 50. The method of claim 48, wherein processing the requested
2 transaction includes:

3 verifying the digital credential; and

4 communicating a result of the verification to the
5 credential service.

1 51. The method of claim 48 further including receiving a
2 activity report from the central service, wherein the
3 activity report lists the transaction information for
4 each digital credential.

1 52. The method of claim 48, wherein the transaction
2 information includes at least one of a message that was
3 signed, a transaction value, an online service, an
4 internet protocol (IP) address, a value of the
5 transaction, a date of the transaction and a the time of
6 the transaction.

3 53. A method comprising:

4 receiving a request from a medical professional to
5 access medical information, wherein the request includes
6 a digital credential for the medical professional;

7 communicating transaction information describing the
8 access request and the digital credential to a credential
9 verification service;

10 receiving a verification result from the credential
11 verification service;

12 providing the medical professional access to the
13 medical information based on the verification result; and

14 receiving an activity report from the credential
15 verification service, wherein the activity report list
16 the transaction information, the digital credential and
17 the transaction result.

1 54. The method of claim 53, wherein the transaction

2 information includes at least an access type, a date of
3 the transaction and a time of the transaction.

1 55. The method of claim 53, further wherein the digital

2 credential was provided by a credential issuing service
3 and a credential service provider.

1 56. The method of claim 53, and further including:
2 receiving a request to access the activity report
3 from an owner of the digital credential; and
4 providing the owner access to the activity report.

DIGITAL CREDENTIAL USAGE REPORTING

ABSTRACT

An credential verification service (CVS) authenticates
5 digital credentials, such as, digital certificates, at the
request of online service providers. The CVS stores the
authentication results and transaction information in a
central activity log. The transaction information can include
a size of the transaction, the online service requesting the
10 authentication, an internet protocol (IP) address of a
computing device originating the transaction and the goods or
services involved in the transaction. The CVS generates an
activity report from the activity log that lists the
authentication results and the transaction information. A
15 fraud detection module within the CVS analyzes the activity
log to identify any unusual patterns in order to identify
fraudulent activities or general misuse of the digital
credential.

60015071.doc

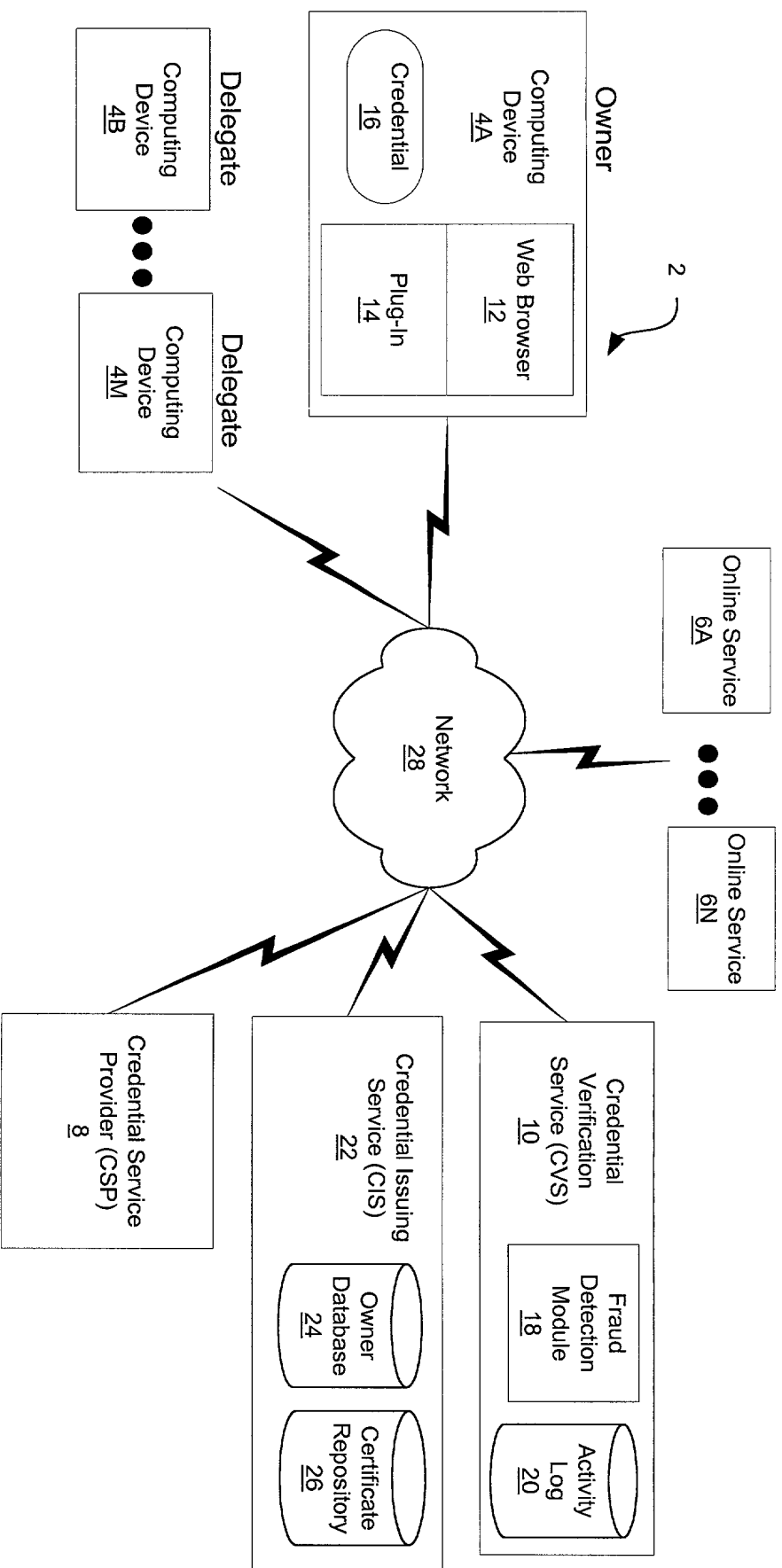


FIG. 1

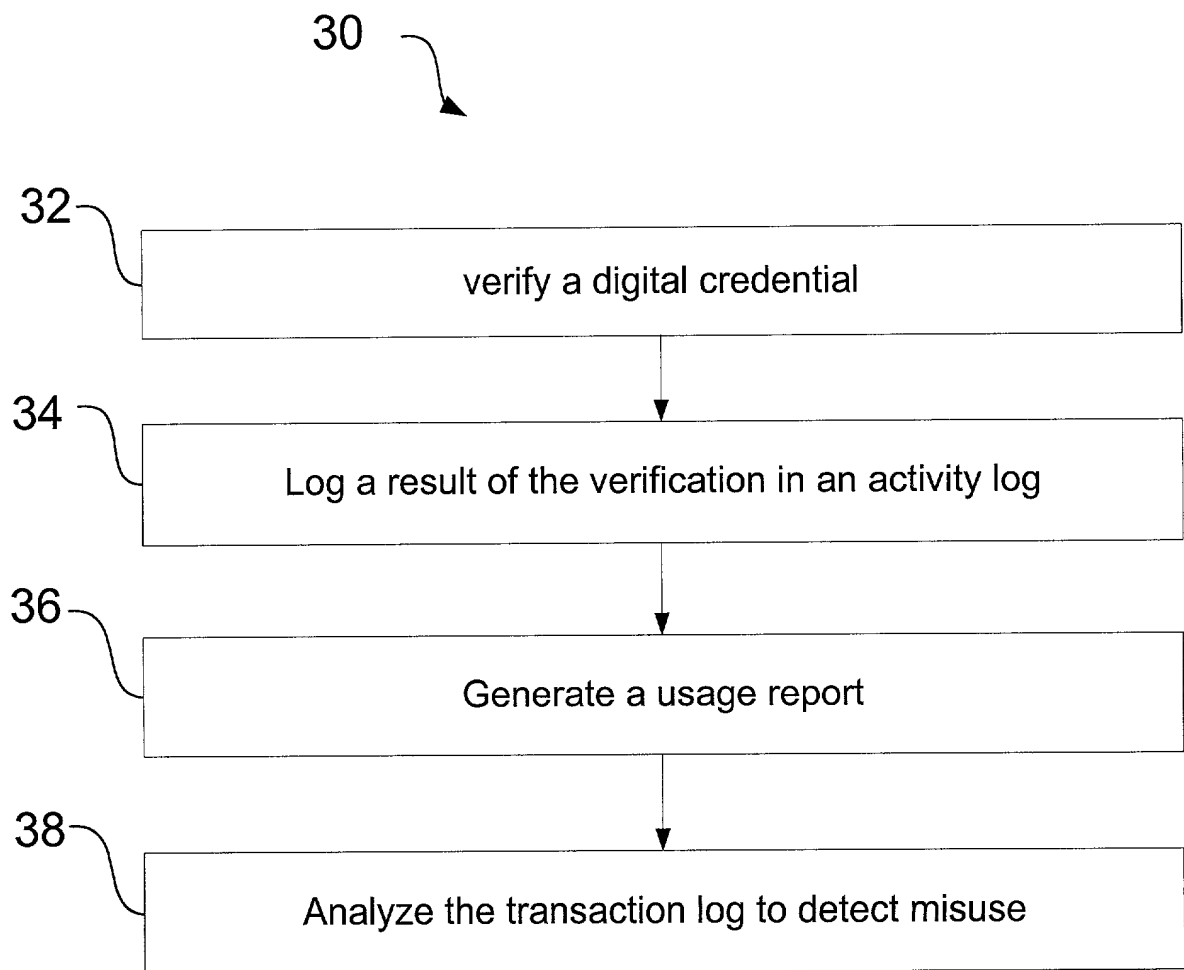


FIG. 2

Activity Log

May 2000

Digital Certificate 1.234.5.6778.9***Jon Smith (Primary Owner)***

10/15/99	10:02 AM	<u>www.amazon.com</u>	Office	\$15.25	Approved
10/15/99	11:04 AM	<u>www.ebay.com</u>	Office	\$100.25	Approved
10/15/99	09:36 PM	<u>www.amazon.com</u>	Home	\$56.65	Approved
10/15/99	04:32 PM	<u>www.etoys.com</u>	Portable	\$25.65	Approved

Susan Johnson (Delegate)

10/15/99	10:02 AM	<u>www.healthcare.com</u>	Work	document accessed	Approved
10/15/99	10:05 AM	<u>www.healthcare.com</u>	Work	document submitted	Approved
10/15/99	10:08 AM	<u>www.healthcare.com</u>	Work	document accessed	Approved
10/15/99	10:09 AM	<u>www.healthcare.com</u>	Work	document accessed	Approved

Albert White (Delegate)

10/15/99	07:42 AM	<u>www.healthcare.com</u>	Work	document accessed	Approved
10/15/99	11:07 AM	<u>www.bankone.com</u>	Work	transfer \$1,000	Rejected

FIG. 3

100

[illegible]